We Claim:

1. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender,

transmitting the message from the server to the recipient, and

the message including a pixel for indicating the opening of the message at the recipient at the server,

providing an encrypted hash of the message, including the indication of the opening of the message at the recipient, at the server, and

transmitting the message, including the indication of the opening of the message at the recipient, and the encrypted hash to the sender.

2. A method as set forth in claim 1, including the steps at the server of:

receiving at the server the message, including the indication of the opening of the message at the recipient and the encrypted hash of the message, and

determining the authenticity of the message, including the opening of the message at the recipient, on the basis of the hash of the message, including the indication of the opening of the message at the recipient, and the hash decrypted from the encrypted hash.

3. A method as set forth in claim 1, including the steps at the server of:

receiving from the sender the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient,

hashing the message, including the indication of the opening of the message the recipient, to provide a first digital fingerprint of the message including the indication of the opening of the message at the recipient,

decrypting the encrypted hash of the message, including the indication of the message at the recipient, to provide a second digital fingerprint of the message including the indication of the opening of the message at the recipient, and

comparing the first and second digital fingerprints to determine the authenticity of the message including the indication of the opening of the message at the recipient.

4. A method as set forth in claim 3, including the steps at the server of:

indicating to the sender the results of the comparison, and

disposing of the message, and including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, when the message and the encrypted hash are transmitted by the server to the sender.

5. A method as set forth in claim 1 wherein

the server receives the message from the sender through the internet,

the server transmits the message to the recipient through the internet,

the server receives the message, including the indication of the opening of the message the recipient, through the internet, and

the server transmits the message, including the indication of the opening of the message at the recipient, through the internet to the sender.

6. A method as set forth in claim 5 wherein

the server indicates the results of the compression to the sender through the internet and wherein

the server disposes of the message, including the indication of the opening of the message at the internet, and the encrypted hash of the message, including the indication of the

opening of the message, when the message and the encrypted hash are transmitted by the server to the sender through the internet.

7. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender,

transmitting the message from the server to the recipient,

the message including a pixel for indicating the opening of the message at the recipient,

receiving the message, including the indication of the opening of the message the recipient, at the server,

receiving an attachment including an indication of the interim stations which receive the message during the transmission of the message from the server to the recipient and back to the server,

providing encrypted hashes of the message, including the indication of the opening of the message at the recipient, and the attachment, and

transmitting to the sender the message, including the indication of the opening of the message the recipient, and the attachment, and the encrypted hashes of the message, including the opening of the message at the recipient, and the attachment.

8. A method as set forth in claim 7, including the steps at the server of:

receiving at the server the message, including the indication of the opening of the message at the recipient, the attachment and the encrypted hashes of the message, including the indication of the opening of the message at the recipient, and the attachment, and

determining the authenticity of the message, including the opening of the message at the recipient, on the basis of the hash of the messages, including the indication of the opening of the message at the recipient, and the hash decrypted from the encrypted hash and the

authenticity of the attachment on the basis of the hashed attachment and the hash decrypted from the encrypted hash of the attachment.

9. A method as set forth in claim 7, including the steps at the server of:

reviewing from the sender the message, including the indication of the opening of the message at the recipient, the encrypted hash of the message, including the indication of the opening of the message at the reception, the attachment and the encrypted hash of the attachment,

hashing the message, including the indication of the opening of the message the recipient, and the attachment to provide first digital fingerprints of the message, including the indication of the opening of the message at the recipient and the attachments,

decrypting the encrypted hash of the message, including the indication of the opening of the message at the recipient, and the attachment to provide second digital fingerprints of the message, including the indication of the opening of the message at the recipient and the attachment, and

comparing the first and second digital fingerprints of the message, including the indication of the opening of the message at the recipient, to determine the authenticity of the message, including the indication of the opening of the message at the recipient and first and second fingerprints of the attachment to determine the authenticity of the attachment.

10. A method as set forth in claim 9, including the steps at the server of:

indicating to the sender the results of the comparisons, and

disposing of the message, including the indications of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, and the attachment and encrypted hash of the attachment when the message, the attachment and the encrypted hashes are transmitted by the server to the sender.

11. A method as set forth in claim 10 wherein

the server receives the message from the sender through the internet and wherein

the server transmits the message to the recipient through the internet and wherein

the server reserves the message, including the indication of the opening of the message at the recipient, to the recipient through the internet and wherein

the server transmits the message through the internet to the sender.

12. A method as set forth in claim 11 wherein

the server indicates the results of the comparison to the sender through the internet and wherein

the server disposes of the message, the attachment and the encrypted hashes of the message and the attachment when the message and the encrypted hash are transmitted by the server to the sender through the internet.

13. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at server of:

receiving the message at the server from the sender,

transmitting the message from the server to the recipient,

the message including a pixel for indicating the opening of the message at the recipient,

receiving the message, including the indication of the interim stations which receive the message during the transmission of the message from the server to the recipient and back to the server,

providing an encrypted hash of the combination of the message and the attachment,

transmitting to the sender the message and the attachment and the encrypted hash of the combination of the message and the attachment.

14. A method as set forth in claim 13 including the steps at the server of:

receiving the message, the attachment and the encrypted hash of the combination of the message and the attachment from the sender,

hashing the combination of the message and the attachment to provide a first digital fingerprint and decrypting the encrypted hash of the combination of the message and the attachment to form a second digital fingerprint, and

determining the authenticity of the message and the attachment on the basis of the first and second digital fingerprints.

15. A method as set forth in claim 13, including the steps at the server of:

receiving from the sender the message, the attachment and the encrypted hash of the combination of the message and the attachment,

hashing the combination of the message and the attachment to form a first digital fingerprint and decrypting the encrypted hash of the combination of the message and the attachment to form a second digital fingerprint, and

comparing the first and second digital fingerprints to determine the authentications of the message and the attachment.

16. A method as set forth in claim 15, including the steps at the server of:

indicating to the sender the results of the comparison, and

disposing of the message and the attachment and the encrypted hash of the message and the attachment when the message, the attachment and the encrypted hash of the combination of the message and the attachment are transmitted by the server to the sender.

17. A method as set forth in claim 13 wherein

the server receives the message from the sender through the internet and wherein

the server transmits the message to the recipient through the internet and wherein

the server receives the message including the indication of the opening of the message at the recipient, and the attachment from the recipient and wherein

the server transmits the message and the attachment and the hash of the combination of the message and the attachment.

18. A method as set forth in claim 17 wherein

the server indicates the results of the comparison to the sender through the internet and wherein

the server disposes of the message, the attachment and the encrypted hash of the combination of the message and the attachment when the message and the attachment and the encrypted hash are transmitted by the server to the sender through the internet.

19. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the step at the server of:

receiving the message from the sender,

assigning the message a unique identification number,

providing a particular tag which includes a unique identification of the message and the recipient,

transferring a database,

transferring to the database the relationship between the sender and the unique identification of the sender and the relationship between the message and the unique identification of the message,

receiving the message from the recipient with an indication in the message that the message has been opened by the recipient,

extracting the identification of the sender,

extracting the unique identification of the message and the recipient from the data in accordance with the unique identifications of the message and the recipient, and

transmitting to the sender an indication that the message has been opened at the recipient.

20. A method as set forth in claim 19 wherein

there is at least one other addressee in addition to the recipient and wherein

the server assigns a unique identification to the one other addressee and records this unique identification in the database to identify the one other addressee.

21. A method as set forth in claim 19 wherein

the particular format is an HTML format.

22. A method as set forth in claim 19 wherein

the server passes the message to the recipient through the internet and wherein

the server receives the message through the internet with the indication of the opening of the message.

23. A method as set forth in claim 21 wherein

there is at least one other addressee in addition to the recipient and wherein

the server assigns a unique identification to the one other addressee and records this unique identification in the database to identify the one other addressee

the server passes the message to the recipient through the internet and wherein

the server receives the message through the internet with the indication of the opening of the message.